Operationalizing Cyber Security Risk Assessments for the Dams Sector

Kevin Burns, Jason Dechant, Darrell Morgeson, and Reginald Meeson, Jr.

The Problem

The Department of Homeland Security's 2013 National Infrastructure Protection plan sets forth goals for a national, coordinated effort to strengthen security and resilience of our nation's critical infrastructure against both physical and cyber threats. The plan challenges the community to consider both physical and cyber security in an integrated, rather than separate, manner.

To evaluate vulnerability to the postulated threat, it is necessary ... to describe the defenses onsite that can be used to mitigate potential vulnerabilities.

Background

In 2005, under DHS sponsorship, IDA initiated the development of the Common Risk Model (CRM) for evaluating and comparing risks associated with the nation's critical infrastructure. This model incorporates commonly used risk metrics that are designed to be transparent and mathematically justifiable. It also enables comparisons of risks to critical assets within and across critical infrastructure sectors.

IDA has continued to develop this model in collaboration with the U.S. Army Corps of Engineers (USACE). The extended model—the Common Risk Model for Dams (CRM D)—takes into account the unique features of dams and navigation locks and provides a systematic approach for evaluating and comparing risks from terrorist threats across a portfolio of dam projects.

In the CRM-D, risk is considered as a function of three variables: threat (T), vulnerability (V), and consequences (C):

$$R = f(T, V, C). \quad (1)$$

The three variables are defined as follows: threat—the probability of a specific attack scenario being attempted by the adversary, given an attack on one of the targets in the portfolio under assessment, denoted as P(A); vulnerability—the probability of defeating the target's defenses, given that the attack is attempted, denoted as P(S|A); and consequences—the estimated loss in terms of human life or economic damage given that the target's defenses are defeated, denoted as C.

The CRM-D calculates risk as the product of these three variables:

$$R = P(A) \times P(S|A) \times C. \quad (2)$$

CRM-D also defines conditional risk (RC) as risk for the attack scenario, given that this scenario is chosen:

$$RC = P(S|A) \times C. \quad (3)$$

The consequence and risk metrics currently considered in the CRM-D are loss of life (LOL) and total economic impacts.

Cyber Security Module of the CRM-D

The National Infrastructure Protection Plan (Department of Homeland Security 2013) set forth goals for a national, coordinated effort to strengthen the security and resilience of our nation's critical infrastructure against human, physical, and cyber threats. It outlines a coordinated risk management framework to secure the cyber elements of critical infrastructure in an integrated fashion with physical security, rather than as a separate consideration.

To support this goal at USACE-maintained dams, IDA, in collaboration with USACE, developed a cyber-risk model focused on cyber attacks against industrial control systems (ICS) that regulate critical dam functions. This model, the Common Risk Model for Dams Cybersecurity Module (CRM-D CSM), enables the assessment of cyber risks and assists in the identification of control systems where stronger cybersecurity defenses are needed to reduce risks to an acceptable level.

The CRM-D CSM is consistent with the Risk Management Framework (RMF) defined by the Committee on National Security Systems Instruction (CNSSI) Policy No. 22 (Committee on National Security Systems 2016) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 (National Institute of Standards and Technology 2011). The CRM-D CSM is intended to complement current processes and give USACE the capability to quickly assess the status of cybersecurity at dams and to move to adopt stronger cyber-defense measures, where needed, in accordance with risk estimates. Risk in the CRM-D CSM depends on the cyber attack chosen and is therefore determined by cyber vulnerability and consequences given a successful cyber attack. The following sections discuss how vulnerability, consequences, and risk are estimated in the CRM-D CSM.

Estimating Vulnerability

Cyber vulnerability is defined as the likelihood of defeating cyber defenses, given a cyber attack. To evaluate vulnerability to the postulated threat, it is necessary to characterize the architecture of the ICS at the dam project and to describe the defenses onsite that can be used to mitigate potential vulnerabilities. These architectures provide different levels of protection against cyber attacks.

ICS configurations have been classified into four system architecture categories representative of USACE dams:

- Platform Information Technology (PIT) System Restricted Interconnection. Refers to a system connected to a project owned by an entity external to USACE.
- PIT System Closed-Restricted. A set of multiple interconnected

systems capable of enabling remote operations.

- PIT System. A system with no external connections.
- PIT Product. The simplest control system with minimal computing resources.

In addition to the system architecture, a number of cyber defense packages with increasingly strong levels of cyber protection have been defined. The CRM-D CSM considers a total of six different cyber defense package levels, ranging from the fewest or most ineffective controls (Cyber Defense Package 0) to the most stringent controls (Cyber Defense Package 5). These cyber defense packages comprise physical defenses, personnel measures, and cyber controls. Physical defenses may include elements such as gates, access controls, and surveillance systems; typical personnel measures include background checks and cybersecurity training; and some cyber controls involve computer access controls and system monitoring. Defense package 0 offers no effective cybersecurity for a dam. Defense package 1 has the minimal number of cyber security measures to receive any credit for having a viable cyber defense. Succeeding defense packages are built on previous defense packages. For example, defense package 2 contains all of the security measures in defense package 1 plus additional measures. Thus, defense packages with greater numerical designations always contain more security measures than those with lesser numerical designations.

Table 1 shows qualitative assessments of cyber vulnerability or the likelihood that a given cyber

Table 1. Cyber Vulnerability Rating for High-End Adversaries

CYBER DEFENSE PACKAGE	SYSTEM ARCHITECTURE			
	PIT SYSTEM RESTRICTED INTERCONNECTION	PIT SYSTEM CLOSED RESTRICTED	PIT SUBSYSTEM	PIT PRODUCT
DEFENSE PACKAGE 5	Very Low			
DEFENSE PACKAGE 4	Low	Very Low	Extremely Low	
DEFENSE PACKAGE 3	Moderate	Low	Very Low	
DEFENSE PACKAGE 2	High	Moderate	Low	Extremely Low
DEFENSE PACKAGE 1	Very High	High	Moderate	Low
DEFENSE PACKAGE 0	Extremely High	Extremely High	Extremely High	Extremely High

Note: The gray cells are not relevant; the defense package-system architecture pairing is unlikely to be encountered or impractical to implement because it would not result in any further risk reduction.

attack, if attempted, will be successful in defeating cyber defenses (also known as the vulnerability or P(S|A)). These estimates were developed by subject matter experts (SMEs) who were considering a high-capability adversary. The resulting likelihoods that these defense configurations would defeat a cyber attack are shown in Table 1. The cyber vulnerability of critical dam functions at any dam site can be determined from its ICS architecture and the level of cyber-defense measures (defense package level) that have been implemented.

Estimating Consequences

Six critical functions can be performed at a dam, and any or all of them can be at risk: (1) flood risk management, (2) hydropower generation, (3) navigation, (4) water supply, (5) water management, and (6) safety. With the exception of water management and safety,[1] a cyber attack from a high-capability adversary can cause damage and consequences when directed against these critical functions.

The USACE Critical Infrastructure Cyber-Security Center of Excellence (CICSCX) maintains and provides a set of rule-based cyber scenarios that includes damage estimates for successful cyber attacks. Using these rules, project personnel choose applicable scenarios for their dams to determine potential damages (e.g., if hydropower governors are cyber vulnerable, then generators and turbines could be destroyed in a cyber attack). Potential damages include destruction of critical items (e.g., generators, locks) and loss of critical functions for an estimated period of time (e.g., a hydropower loss for 36 hours). All rule-based scenarios that are applicable are evaluated for consequences and risk.

The consequence estimation team provides consequence estimates in terms of lives lost and economic loss for each applicable scenario at a dam. Tables such as Table 2 are used to produce semi-quantitative estimates for consequences—Level 1 (lowest) to Level 5 (highest)—for the identified scenarios at the dam. These estimates are used in determining risk for lives lost and for economic loss, and they provide an informed basis for determining risk mitigation

Table 2. Consequence Scale Based on Loss-of-Life (LOL) Estimation

Lives Lost Consequence Ratings				
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
0	0 < LOL ≤ 50	50 < LOL ≤ 100	100 < LOL ≤ 200	> 200

[1] Water management and safety are functions that are not considered to cause immediate consequences as a result of a cyber-attack. More sophisticated attack vectors executed over a longer period of time could cause damage to these two critical functions. USACE chose not to consider those attacks at this point.

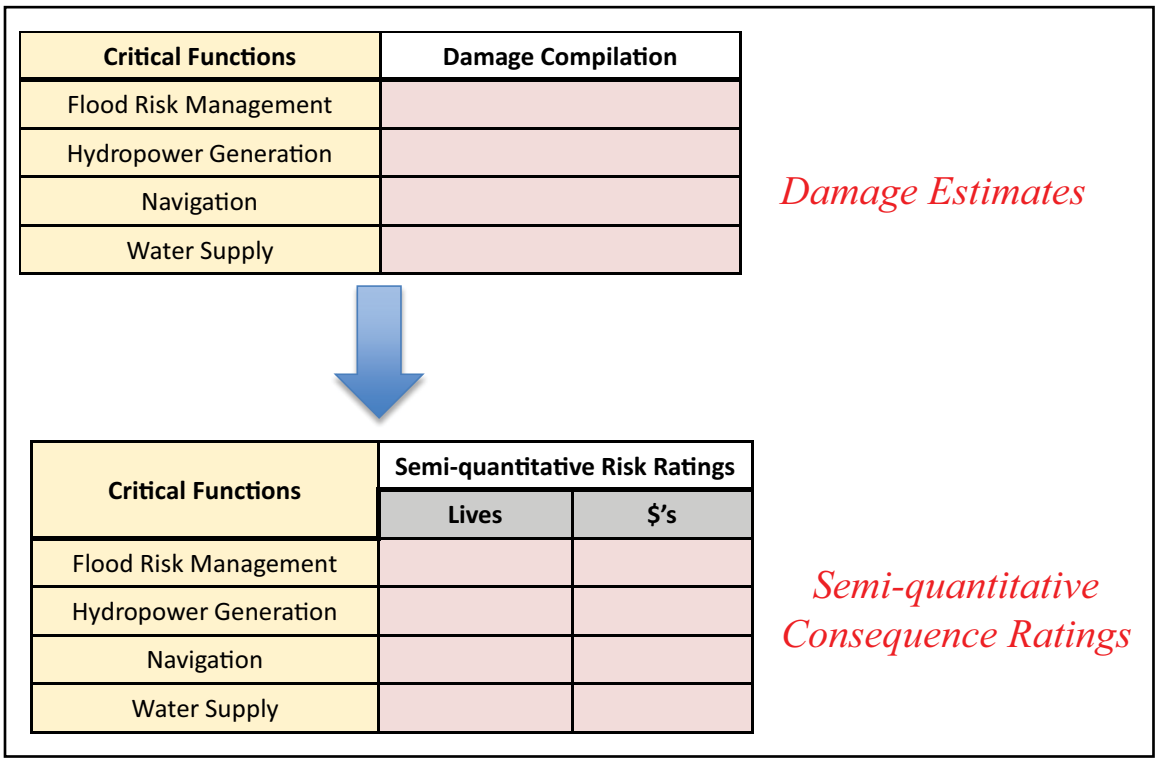


Figure 1. Consequence Estimation Process

measures. Table 2 is used to estimate consequences in terms of loss of life. A similar table is used for estimating economic loss. Figure 1 illustrates the consequence estimation process.

Estimating Risk

Risk is based on combining cyber vulnerability and consequences given a successful cyber attack. A high-capability adversary who can potentially breach the cyber defenses at the dam is assumed for estimating vulnerability and consequences. Given that these defenses are breached, the adversary has the capability to take control of the critical functions linked to the ICS to achieve maximum consequences. All of the damages and consequences analyzed for each ICS are calculated for each applicable scenario identified by dam project personnel and the CICSCX.

Table 3 shows how to estimate cyber risk for ICSs associated with dams. By combining the vulnerability rating with the corresponding consequence rating (either loss of life or economic loss), a qualitative risk rating associated with each combination of vulnerability and consequence ratings is assigned, ranging from "Very Low" to "Very High."

Once a risk estimate has been generated, an analyst can determine what improvements to cyber defenses, if any, are required. For example, consider a dam project with a PIT System Closed Restricted architecture and Cyber Defense Package 1. Also suppose that the consequences for a particular critical function have been estimated as Level 4. This pairing results in a vulnerability rating of

Table 3. ICS Cyber Risk Rating

VULNERABILITY RATING	CONSEQUENCE RATING				
	LEVEL1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
EXTREMELY HIGH	Very Low	Low	High	Very High	Very High
VERY HIGH	Very Low	Low	Moderate	Very High	Very High
HIGH	Very Low	Low	Moderate	High	Very High
MODERATE	Very Low	Low	Moderate	Moderate	High
LOW	Very Low	Low	Low	Low	Moderate
VERY LOW	Very Low	Very Low	Low	Low	Low
EXTREMELY LOW	Very Low	Very Low	Very Low	Low	Low

"high" and therefore a risk rating of "high," as shown in Figure 2. If the CICSCX risk tolerance is "moderate" or below, to reach an acceptable level of risk, the dam should adopt Cyber Defense Package 2 security measures. This security improvement from Cyber Defense Package 1 to Cyber Defense Package 2 would result in a reduction in risk from "high" to "moderate" and would meet the CICSCX tolerance for acceptable risk, as shown in Figure 2.

Conclusion

The CRM-D CSM is easily implemented and can be used to develop a concise report for cyber risk at dams. Risk, as defined by the CRM-D CSM, is based on combining cyber vulnerability (i.e., the likelihood of a successful cyber attack given that the attack is attempted) with consequences given a successful cyber attack. Consequences are produced by outcomes that adversely affect one or more of the dam's critical functions: (1) flood risk management; (2) hydropower generation; (3) navigation; and (4) water supply. Vulnerability and consequences are estimated using qualitative and semi-quantitative scales ranging from "extremely low" to "extremely high" for vulnerability and "very low" to "very high" for consequences.

Risk is estimated as a function of consequences and vulnerability. Vulnerability estimates are elicited as likelihoods of successful attacks by a specific adversary. The elicited estimates can then be used to estimate the vulnerability of a target that is protected by any combination of the generic security configurations against any of the reference attack vectors for the adversary groups under consideration. This methodology, which was developed by IDA in a collaborative effort with USACE and

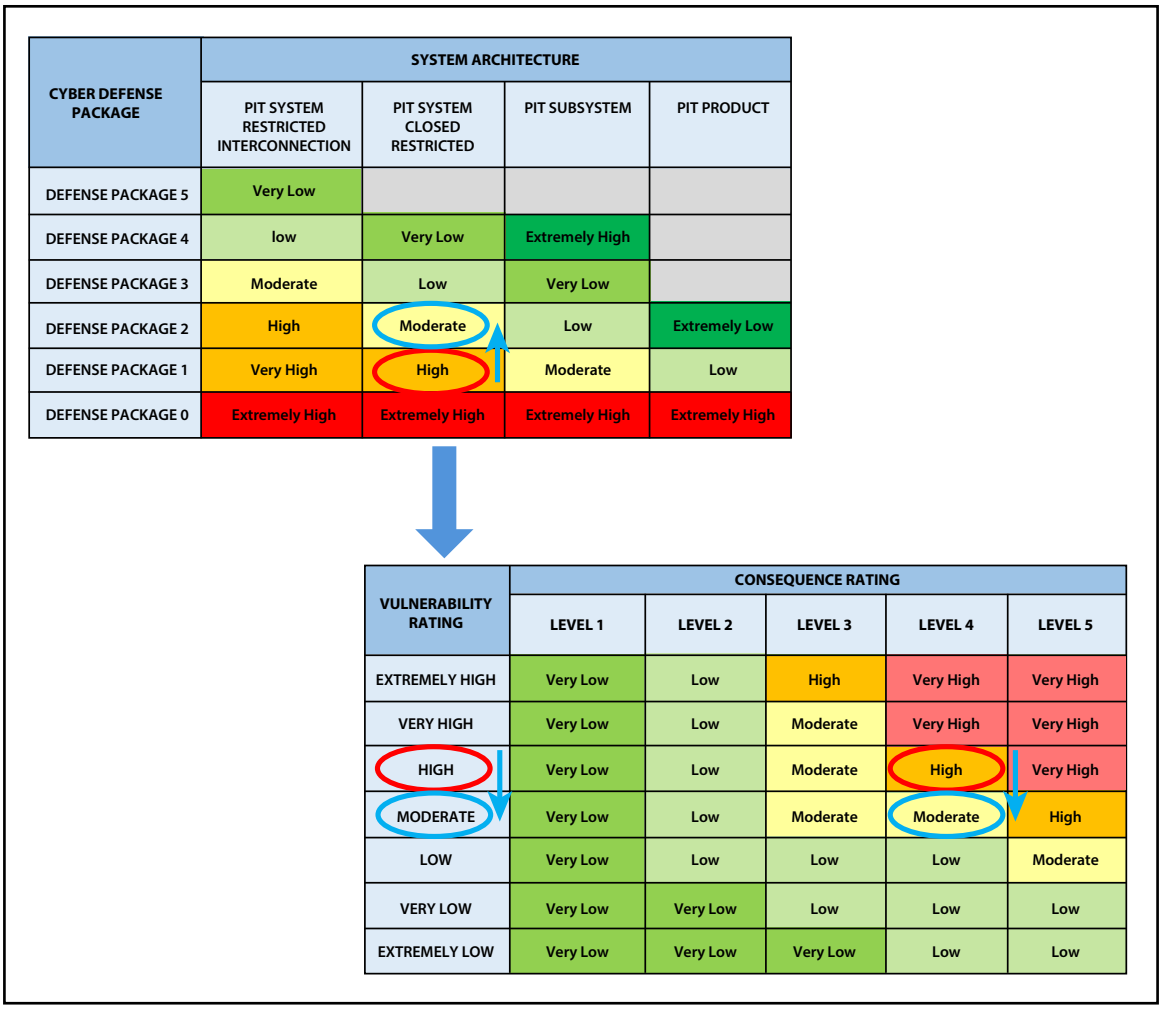


Figure 2. Reducing Risk by Reducing Vulnerability

the Department of Homeland Security (DHS), provides a systematic approach for evaluating and comparing cybersecurity risks across a large portfolio of dams. The CRM-D CSM can effectively show the benefits of implementing a particular risk mitigation strategy.

The various components of CRM-D, in addition to the CRM-D CSM, provide risk analysts a suite of rigorous tools for estimating physical and cyber security risks across a portfolio of dams. The results from a CRM-D risk assessment can be used to inform investment decisions to mitigate those risks and enhance the security posture at our nation's critical infrastructure against potential adversaries.

References

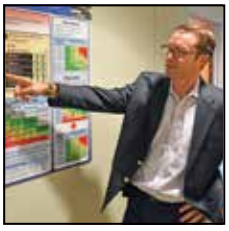
Committee on National Security Systems. 2016. *Cybersecurity Risk Management.* CNSSP 22. Fort Meade, MD: National Security Agency, CNSS Secretariat (1E414), August.

Department of Homeland Security. 2013. *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilienc*e. Washington, DC: Department of Homeland Security.

National Institute of Standards and Technology. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View.* NIST Special Publication 800-39. Gaithersburg, MD: National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, March.

Dr. Kevin Burns *is an Adjunct Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Doctor of Philosophy in operations research from the University of Georgia.*

Dr. Jason Dechant *is a Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Doctor of Philosophy in public policy from George Mason University.*



Mr. Darrell Morgeson *is an Adjunct Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Master of Science in operations research from the Naval Postgraduate School.*

Dr. Reginald Meeson *is a Research Staff Member in IDA's Information Technology and Systems Division. He holds a Doctor of Philosophy in electrical and computer engineering from the University of California, Santa Barbara.*